

IN THE SPECIFICATION

Please replace the paragraph beginning at page 10, line 20 with the following rewritten paragraph:

B1 ¶ In accordance with the present invention, deleting a secure file may not be an atomic operation because it would be undesirable to allow clients the ability to delete a secure file unless the client was authorized to do so. Delete operations must be able to differentiate between files that should be able to be deleted (non-secure files and secure files being deleted by an authorized client) and those that should not be able to be deleted (secure files attempted to be deleted by an unauthorized client). Therefore, the atomic delete operation must be designed to check the fixed file security status of a file before deleting it. Only files with an associated fixed file security status of type "operations allowed" will be deleted atomically. A new apparatus and method has been developed for the deletion of a secure file. ~

Please replace the paragraph beginning at page 12, line 4 with the following rewritten paragraph:

B2 ¶ The set delete-on-close request may also be used to delete non-secure files, though the atomic delete operation is available and easier. However, there is no need for validation in this case. ~

IN THE CLAIMS

Please amend claims 6, 10, 11, and 13 as follows:

B3 6. (Amended Once) The method of claim 5, wherein the apparatus has a third memory associated with the file, said third memory storing a delete-on-close status, said third memory initially storing a first value and changeable to a second value wherein said first value indicates